

SC-200 Dumps

Microsoft Security Operations Analyst

<https://www.certleader.com/SC-200-dumps.html>



NEW QUESTION 1

- (Exam Topic 1)

The issue for which team can be resolved by using Microsoft Defender for Office 365?

- A. executive
- B. marketing
- C. security
- D. sales

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb-and-teams?view=o365-worldwide>

NEW QUESTION 2

- (Exam Topic 1)

You need to implement Azure Sentinel queries for Contoso and Fabrikam to meet the technical requirements. What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:	<div><div></div><div>▼</div><div>0</div><div>1</div><div>2</div><div>3</div></div>
Query element required to correlate data between tenants:	<div><div></div><div>▼</div><div>extend</div><div>project</div><div>workspace</div></div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants>

NEW QUESTION 3

- (Exam Topic 1)

The issue for which team can be resolved by using Microsoft Defender for Endpoint?

- A. executive
- B. sales
- C. marketing

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-ios>

NEW QUESTION 4

- (Exam Topic 2)

You need to configure DC1 to meet the business requirements.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Provide domain administrator credentials to the litware.com Active Directory domain.

Create an instance of Microsoft Defender for Identity.

Provide global administrator credentials to the litware.com Azure AD tenant.

Install the sensor on DC1.

Install the standalone sensor on DC1.

Answer Area

⬅️⬆️

➡️⬆️

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Text Description automatically generated with medium confidence
Step 1: log in to <https://portal.atp.azure.com> as a global admin Step 2: Create the instance
Step 3. Connect the instance to Active Directory Step 4. Download and install the sensor. Reference:
<https://docs.microsoft.com/en-us/defender-for-identity/install-step1> <https://docs.microsoft.com/en-us/defender-for-identity/install-step4>

NEW QUESTION 5

- (Exam Topic 2)
You need to implement Azure Defender to meet the Azure Defender requirements and the business requirements.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Log Analytics workspace to use:

A new Log Analytics workspace in the East US Azure region

Default workspace created by Azure Security Center

LA1

Windows security events to collect:

All Events

Common

Minimal

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application Description automatically generated

NEW QUESTION 6

- (Exam Topic 3)
You have a Microsoft Sentinel workspace named Workspace1.
You need to exclude a built-in, source-specific Advanced Security information Model (ASIM) parse from a built-in unified ASIM parser.
What should you create in Workspace1?

- A. a watch list
- B. an analytic rule
- C. a hunting query
- D. a workbook

Answer: A

NEW QUESTION 7

- (Exam Topic 3)
You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.
You need to deploy the log forwarder.
Which three actions should you perform in sequence? To answer, move the appropriate actions form the list of actions to the answer area and arrange them in the correct order.

Actions

Answer Area

Deploy an OMS Gateway on the network.

Set the syslog daemon to forward the events directly to Azure Sentinel.

Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

Download and install the Log Analytics agent.

Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog>

NEW QUESTION 8

- (Exam Topic 3)

You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2. The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Security Center tab.)



Resource exemption (preview)

< Now you can exempt irrelevant resources so they do not affect your secure score. >
[Learn more](#)

Each security control below represents a security risk you should mitigate. Address the recommendations in each control, focusing on the controls worth the most points. To get the max score, fix all recommendations for all resources in a control. [Learn more](#) >

Search recommendations: Control status: **2 Selected** Recommendation status: **2 Selected**
Recommendation maturity: **All** Resource type: **All** Quick fix available: **All**
Contains exemptions: **All** [Reset filters](#) Group by controls: ☒ On

Controls	Potential score increase	Unhealthy resources	Resource Health
> Restrict unauthorized network access	+9% (4 points)	2 of 2 resources	<div><div></div></div>
> Secure management ports	+9% (4 points)	1 of 2 resources	<div><div></div></div>
> Enable encryption at rest	+9% (4 points)	2 of 2 resources	<div><div></div></div>
> Remediate security configurations	+4% (2 points)	1 of 2 resources	<div><div></div></div>
> Apply adaptive application control	+3% (2 points)	1 of 2 resources	<div><div></div></div>
> Apply system updates Completed	+0% (0 points)	None	<div><div></div></div>
> Enable endpoint protection Completed	+0% (0 points)	None	<div><div></div></div>
> Remediate vulnerabilities Completed	+0% (0 points)	None	<div><div></div></div>
> Implement security best practices Completed	+0% (0 points)	None	<div><div></div></div>
> Enable MFA Completed	+0% (0 points)	None	<div><div></div></div>
> Manage access and permissions Completed	+0% (0 points)	None	<div><div></div></div>

Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Policies tab.)

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	<input type="radio"/>	<input type="radio"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="radio"/>	<input type="radio"/>
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-ac> <https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1>

NEW QUESTION 9

- (Exam Topic 3)

You have five on-premises Linux servers.

You have an Azure subscription that uses Microsoft Defender for Cloud. You need to use Defender for Cloud to protect the Linux servers.

What should you install on the servers first?

- A. the Dependency agent
B. the Log Analytics agent
C. the Azure Connected Machine agent
D. the Guest Configuration extension

Answer: B

Explanation:

Defender for Cloud depends on the Log Analytics agent. Use the Log Analytics agent if you need to:

* Collect logs and performance data from Azure virtual machines or hybrid machines hosted outside of Azure

* Etc. Reference:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/os-coverage>

<https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview#log-analytics-agent>

NEW QUESTION 10

- (Exam Topic 3)

You are investigating an incident in Azure Sentinel that contains more than 127 alerts. You discover eight alerts in the incident that require further investigation.

You need to escalate the alerts to another Azure Sentinel administrator. What should you do to provide the alerts to the administrator?

- A. Create a Microsoft incident creation rule
- B. Share the incident URL
- C. Create a scheduled query rule
- D. Assign the incident

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases>

NEW QUESTION 10

- (Exam Topic 3)

You have a Microsoft subscription that has Microsoft Defender for Cloud enabled. You configure the Azure logic apps shown in the following table.

Name	Trigger	Action
LogicApp1	When a Defender for Cloud recommendation is created or triggered	Send an email
LogicApp2	When a Defender for Cloud alert is created or triggered	Send an email

You need to configure an automatic action that will run if a Suspicious process executed alert is triggered. The solution must minimize administrative effort. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Configure the Suppress similar alerts settings.

Configure the Mitigate the threat settings.

Filter by alert title.

Select **Take action**.

Configure the Prevent future attacks settings.

Configure the Trigger automated response settings.

>

<

Answer Area

1

2

3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- * A. Configure the Trigger automated response settings in the Azure Security Center or Azure Logic App,
- * B. Filter by alert title (e.g. "Suspicious process executed").
- * C. Select "Take action" (e.g. "Mitigate the threat").

NEW QUESTION 12

- (Exam Topic 3)

You recently deployed Azure Sentinel.

You discover that the default Fusion rule does not generate any alerts. You verify that the rule is enabled. You need to ensure that the Fusion rule can generate alerts.

What should you do?

- A. Disable, and then enable the rule.
- B. Add data connectors
- C. Create a new machine learning analytics rule.
- D. Add a hunting bookmark.

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources>

NEW QUESTION 15

- (Exam Topic 3)

You create a hunting query in Azure Sentinel.

You need to receive a notification in the Azure portal as soon as the hunting query detects a match on the query. The solution must minimize effort.

What should you use?

- A. a playbook
- B. a notebook
- C. a livestream
- D. a bookmark

Answer: C

Explanation:

Use livestream to run a specific query constantly, presenting results as they come in. Reference:
<https://docs.microsoft.com/en-us/azure/sentinel/hunting>

NEW QUESTION 18

- (Exam Topic 3)

You have a third-party security information and event management (SIEM) solution.

You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign-events in near real time.

What should you do to route events to the SIEM solution?

- A. Create an Azure Sentinel workspace that has a Security Events connector.
- B. Configure the Diagnostics settings in Azure AD to stream to an event hub.
- C. Create an Azure Sentinel workspace that has an Azure Active Directory connector.
- D. Configure the Diagnostics settings in Azure AD to archive to a storage account.

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring>

NEW QUESTION 20

- (Exam Topic 3)

You have an Azure Sentinel workspace.

You need to test a playbook manually in the Azure portal. From where can you run the test in Azure Sentinel?

- A. Playbooks
- B. Analytics
- C. Threat intelligence
- D. Incidents

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand>

NEW QUESTION 25

- (Exam Topic 3)

You have a Microsoft Sentinel workspace named workspace1 that contains custom Kusto queries.

You need to create a Python-based Jupyter notebook that will create visuals. The visuals will display the results of the queries and be pinned to a dashboard. The solution must minimize development effort.

What should you use to create the visuals?

- A. plotly
- B. TensorFlow
- C. msticpy
- D. matplotlib

Answer: C

Explanation:

msticpy is a library for InfoSec investigation and hunting in Jupyter Notebooks. It includes functionality to: query log data from multiple sources. enrich the data with Threat Intelligence, geolocations and Azure resource data. extract Indicators of Activity (IoA) from logs and unpack encoded data.

MSTICPy reduces the amount of code that customers need to write for Microsoft Sentinel, and provides:

Data query capabilities, against Microsoft Sentinel tables, Microsoft Defender for Endpoint, Splunk, and other data sources.

Threat intelligence lookups with TI providers, such as VirusTotal and AlienVault OTX.

Enrichment functions like geolocation of IP addresses, Indicator of Compromise (IoC) extraction, and WhoIs lookups.

Visualization tools using event timelines, process trees, and geo mapping.

Advanced analyses, such as time series decomposition, anomaly detection, and clustering. Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/notebook-get-started> <https://msticpy.readthedocs.io/en/latest/>

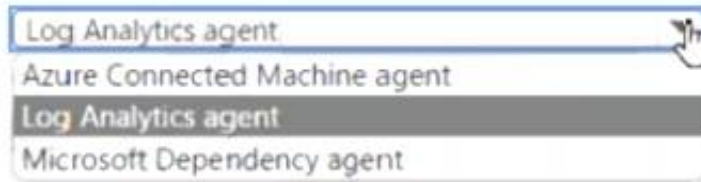
NEW QUESTION 26

- (Exam Topic 3)

Your on-premises network contains 100 servers that run Windows Server. You have an Azure subscription that uses Microsoft Sentinel.

You need to upload custom logs from the on-premises servers to Microsoft Sentinel. What should you do? To answer, select the appropriate options in the answer area.

On the servers, install the:



Configure custom log settings by using the:



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To upload custom logs from the on-premises servers to Microsoft Sentinel, you should install the Log Analytics agent on each of the 100 servers. The Log Analytics agent is a lightweight agent that runs on the server and allows it to connect to the cloud-based Microsoft Defender Security Center. Once installed, the agent will allow the Microsoft Sentinel service to collect and analyze the custom log data from the servers.

NEW QUESTION 27

- (Exam Topic 3)

You plan to create a custom Azure Sentinel query that will provide a visual representation of the security alerts generated by Azure Security Center. You need to create a query that will be used to display a bar graph. What should you include in the query?

- A. extend
- B. bin
- C. count
- D. workspace

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-chart-visualizations>

NEW QUESTION 30

- (Exam Topic 3)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center. Solution: From Regulatory compliance, you download the report.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

NEW QUESTION 35

- (Exam Topic 3)

You are investigating an incident by using Microsoft 365 Defender.

You need to create an advanced hunting query to count failed sign-in authentications on three devices named CFOLaptop, CEOLaptop, and COOLaptop.

How should you complete the query? To answer, select the appropriate options in the answer area. NOTE Each correct selection is worth one point

Values	Answer Area
<code> project LogonFailures=count()</code>	
<code> summarize LogonFailures=count() by DeviceName, LogonType</code>	
<code> where ActionType == FailureReason</code>	
<code> where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop")</code>	
<code>ActionType == "LogonFailed"</code>	
<code>ActionType == FailureReason</code>	
<code>DeviceEvents</code>	
<code>DeviceLogonEvents</code>	

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Values	Answer Area
<code> project LogonFailures=count()</code>	
<code> summarize LogonFailures=count() by DeviceName, LogonType</code>	
<code> where ActionType == FailureReason</code>	<code>DeviceLogonEvents</code>
<code> where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop")</code>	<code> where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop")</code> and
<code>ActionType == "LogonFailed"</code>	<code>ActionType == FailureReason</code>
<code>ActionType == FailureReason</code>	<code> summarize LogonFailures=count() by DeviceName, LogonType</code>
<code>DeviceEvents</code>	
<code>DeviceLogonEvents</code>	

NEW QUESTION 40

- (Exam Topic 3)

A company wants to analyze by using Microsoft 365 Apps.

You need to describe the connected experiences the company can use.

Which connected experiences should you describe? To answer, drag the appropriate connected experiences to the correct description. Each connected experience may be used once, more than once, or not at all. You may need to drag the split between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Connected experiences	Answer Area
<div> <input type="text"/> <input type="text"/> <input type="text"/> </div> <div> <input type="text"/> </div>	<div> <div> Description <p>Provides advanced grammar and style refinements such as clarity, conciseness, formality, and vocabulary suggestions.</p> <p>Allows you to use and repurpose existing content from relevant files most often used by coworkers.</p> <p>Identifies how much content in a document is original and inserts citations when necessary.</p> </div> <div> Connected experience <div></div> <div></div> <div></div> </div> </div>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 41

- (Exam Topic 3)

You create a new Azure subscription and start collecting logs for Azure Monitor.

You need to configure Azure Security Center to detect possible threats related to sign-ins from suspicious IP addresses to Azure virtual machines. The solution must validate the configuration.

Which three actions should you perform in a sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.

Actions	Answer Area
Change the alert severity threshold for emails to Medium .	
Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.	
Enable Azure Defender for the subscription.	⬅️
Change the alert severity threshold for emails to Low .	➡️
Run the executable file and specify the appropriate arguments.	⬆️
Rename the executable file as AlertTest.exe.	⬇️

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation>

NEW QUESTION 45

- (Exam Topic 3)

Your company uses Azure Sentinel to manage alerts from more than 10,000 IoT devices.

A security manager at the company reports that tracking security threats is increasingly difficult due to the large number of incidents.

You need to recommend a solution to provide a custom visualization to simplify the investigation of threats and to infer threats by using machine learning.

What should you include in the recommendation?

- A. built-in queries
B. livestream
C. notebooks
D. bookmarks

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

NEW QUESTION 46

- (Exam Topic 3)

A security administrator receives email alerts from Azure Defender for activities such as potential malware uploaded to a storage account and potential successful brute force attacks.

The security administrator does NOT receive email alerts for activities such as antimalware action failed and suspicious network activity. The alerts appear in Azure Security Center.

You need to ensure that the security administrator receives email alerts for all the activities. What should you configure in the Security Center settings?

- A. the severity level of email notifications
- B. a cloud connector
- C. the Azure Defender plans
- D. the integration settings for Threat detection

Answer: A

Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/microsoft-365-defender/get-email-notifications-on-new-incidents-from>

NEW QUESTION 48

- (Exam Topic 3)

You implement Safe Attachments policies in Microsoft Defender for Office 365.

Users report that email messages containing attachments take longer than expected to be received. You need to reduce the amount of time it takes to deliver messages that contain attachments without

compromising security. The attachments must be scanned for malware, and any messages that contain malware must be blocked.

What should you configure in the Safe Attachments policies?

- A. Dynamic Delivery
- B. Replace
- C. Block and Enable redirect
- D. Monitor and Enable redirect

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments?view=o365-world>

NEW QUESTION 52

- (Exam Topic 3)

You have a Microsoft Sentinel workspace named sws1.

You need to create a hunting query to identify users that list storage keys of multiple Azure Storage accounts. The solution must exclude users that list storage keys for a single storage account.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```
| where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| join kind= inner (
    AzureActivity
    | where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
    | where ActivityStatusValue == "Succeeded"
    | project ExpectedIpAddress=CallerIpAddress, Caller
    | evaluate
) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId)
    by OperationNameValue, Caller, CallerIpAddress
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: AzureActivity

The AzureActivity table includes data from many services, including Microsoft Sentinel. To filter in only data from Microsoft Sentinel, start your query with the following code:

Box 2: autocluster()

Example: description: |

'Listing of storage keys is an interesting operation in Azure which might expose additional

secrets and PII to callers as well as granting access to VMs. While there are many benign operations of this

type, it would be interesting to see if the account performing this activity or the source IP address from which it is being done is anomalous.

The query below generates known clusters of ip address per caller, notice that users which only had single operations do not appear in this list as we cannot learn from it their normal activity (only based on a single event). The activities for listing storage account keys is correlated with this learned

clusters of expected activities and activity which is not expected is returned.' AzureActivity

| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"

| where ActivityStatusValue == "Succeeded"

| join kind= inner (AzureActivity

| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"

| where ActivityStatusValue == "Succeeded"

| project ExpectedIpAddress=CallerIpAddress, Caller

| evaluate autocluster()

) on Caller

| where CallerIpAddress != ExpectedIpAddress

| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId)

by OperationNameValue, Caller, CallerIpAddress

| extend timestamp = StartTime, AccountCustomEntity = Caller, IPCustomEntity = CallerIpAddress Reference:

https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/AzureActivity/Anomalous_Listing_O

NEW QUESTION 56

- (Exam Topic 3)

You use Azure Sentinel.

You need to receive an immediate alert whenever Azure Storage account keys are enumerated. Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a livestream
- B. Add a data connector
- C. Create an analytics rule
- D. Create a hunting query.
- E. Create a bookmark.

Answer: BC

Explanation:

B: To add a data connector, you would use the Azure Sentinel data connectors feature to connect to your Azure subscription and to configure log data collection for Azure Storage account key enumeration events.

C: After adding the data connector, you need to create an analytics rule to analyze the log data from the Azure storage connector, looking for the specific event of Azure storage account keys enumeration. This rule will trigger an alert when it detects the specific event, allowing you to take immediate action.

NEW QUESTION 61

- (Exam Topic 3)

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a storage account named storage1. You receive an alert that there was an unusually high volume of delete operations on the blobs in storage1. You need to identify which blobs were deleted. What should you review?

- A. the activity logs of storage1
- B. the Azure Storage Analytics logs
- C. the alert details
- D. the related entities of the alert

Answer: A

Explanation:

To identify which blobs were deleted, you should review the activity logs of the storage account. The activity logs contain information about all the operations that have taken place in the storage account, including delete operations. These logs can be accessed in the Azure portal by navigating to the storage account, selecting "Activity log" under the "Monitoring" section, and filtering by the appropriate time range. You can also use Azure Monitor and Log Analytics to query and analyze the activity logs data.

References:

- <https://docs.microsoft.com/en-us/azure/storage/common/storage-activity-logs>
- <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-log-azure-storage>

NEW QUESTION 66

- (Exam Topic 3)

You are informed of an increase in malicious email being received by users.

You need to create an advanced hunting query in Microsoft 365 Defender to identify whether the accounts of the email recipients were compromised. The query must return the most recent 20 sign-ins performed by the recipients within an hour of receiving the known malicious email.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.


```
let MaliciousEmails =
    | where MalwareFilterVerdict == "Malware"
    | project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails
| join (
    | project LogonTime = Timestamp, AccountName, DeviceName
    ) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
|
select 20
take 20
top 20
```

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application, email Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view>

NEW QUESTION 67

- (Exam Topic 3)

Your company has an on-premises network that uses Microsoft Defender for Identity.

The Microsoft Secure Score for the company includes a security assessment associated with unsecure Kerberos delegation.

You need remediate the security risk. What should you do?

- A. Install the Local Administrator Password Solution (LAPS) extension on the computers listed as exposed entities.
B. Modify the properties of the computer objects listed as exposed entities.
C. Disable legacy protocols on the computers listed as exposed entities.
D. Enforce LDAP signing on the computers listed as exposed entities.

Answer: B

Explanation:

To remediate the security risk associated with unsecure Kerberos delegation, you should modify the properties of the computer objects listed as exposed entities. Specifically, you should set the Kerberos delegation settings to either 'Trust this computer for delegation to any service' or 'Trust this computer for delegation to specified services only'. This will ensure that the computer is not allowed to use Kerberos delegation to access other computers on the network.

Reference: <https://docs.microsoft.com/en-us/windows/security/identity-protection/microsoft-defender-for-iden>

NEW QUESTION 72

- (Exam Topic 3)

You have an Azure subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains two users named User1 and User2.

You plan to deploy Azure Defender.

You need to enable User1 and User2 to perform tasks at the subscription level as shown in the following table.

User	Task
User1	<ul style="list-style-type: none"> Assign initiatives Edit security policies Enable automatic provisioning
User2	<ul style="list-style-type: none"> View alerts and recommendations Apply security recommendations Dismiss alerts

The solution must use the principle of least privilege.

Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all.

You may need to drag the split bar between panes or scroll to view content.

Roles	Answer Area
Contributor	User1: <input type="text"/>
Owner	User2: <input type="text"/>
Security administrator	
Security reader	

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: Owner

Only the Owner can assign initiatives. Box 2: Contributor

Only the Contributor or the Owner can apply security recommendations.

Reference:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions>

NEW QUESTION 74

- (Exam Topic 3)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are configuring Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: You add each account as a Sensitive account. Does this meet the goal?

- A. Yes
B. No

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

NEW QUESTION 78

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription that uses Microsoft SharePoint Online. You delete users from the subscription.

You need to be notified if the deleted users downloaded numerous documents from SharePoint Online sites during the month before their accounts were deleted.

What should you use?

- A. a file policy in Microsoft Defender for Cloud Apps
B. an access review policy
C. an alert policy in Microsoft Defender for Office 365
D. an insider risk policy

Answer: C

Explanation:

Alert policies let you categorize the alerts that are triggered by a policy, apply the policy to all users in your organization, set a threshold level for when an alert is triggered, and decide whether to receive email notifications when alerts are triggered.

Default alert policies include:

Unusual external user file activity - Generates an alert when an unusually large number of activities are performed on files in SharePoint or OneDrive by users outside of your organization. This includes activities such as accessing files, downloading files, and deleting files. This policy has a High severity setting.

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies>

NEW QUESTION 80

- (Exam Topic 3)

You have 50 on-premises servers.

You have an Azure subscription that uses Microsoft Defender for Cloud. The Defender for Cloud deployment has Microsoft Defender for Servers and automatic provisioning enabled.

You need to configure Defender for Cloud to support the on-premises servers. The solution must meet the following requirements:

- Provide threat and vulnerability management.
- Support data collection rules.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
From the Data controller settings in the Azure portal, create an Azure Arc data controller.	1
On the on-premises servers, install the Azure Monitor agent.	2
From the Add servers with Azure Arc settings in the Azure portal, generate an installation script.	3
On the on-premises servers, install the Azure Connected Machine agent.	
On the on-premises servers, install the Log Analytics agent.	

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

To configure Defender for Cloud to support the on-premises servers, you should perform the following three actions in sequence:

- On the on-premises servers, install the Azure Connected Machine agent.
- On the on-premises servers, install the Log Analytics agent.
- From the Data controller settings in the Azure portal, create an Azure Arc data controller.

Once these steps are completed, the on-premises servers will be able to communicate with the Azure Defender for Cloud deployment and will be able to support threat and vulnerability management as well as data collection rules.

Reference: <https://docs.microsoft.com/en-us/azure/security-center/deploy-azure-security-center#on-premises-d>

NEW QUESTION 82

- (Exam Topic 3)

Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant. Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.

You deploy Azure Sentinel to a new Azure subscription.

You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Add the Security Events connector to the Azure Sentinel workspace.
B. Create a query that uses the workspace expression and the union operator.
C. Use the alias statement.
D. Create a query that uses the resource expression and the alias operator.
E. Add the Azure Sentinel solution to each workspace.

Answer: BE

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants>

NEW QUESTION 85

- (Exam Topic 3)

You have the following SQL query.

```
let IPList = _GetWatchlist('Bad_IPs');
Event
| where Source == "Microsoft-Windows-Sysmon"
| where EventID == 3
| extend EvData = parse_xml(EventData)
| extend EventDetail = EvData.DataItem.EventData.Data
| extend SourceIP = EventDetail.[9].["#text"], DestinationIP = EventDetail.[14].["#text"]
| where SourceIP in (IPList) or DestinationIP in (IPList)
| extend IPMatch = case( SourceIP in (IPList), "SourceIP", DestinationIP in (IPList), "DestinationIP", "None")
| extend timestamp = TimeGenerated, AccountCustomEntity = Username, HostCustomEntity = Computer, '
```

Answer Area

Statements	Yes	No
The Username field is set as the account entity.	<input type="radio"/>	<input checked="" type="radio"/>
The watchlist cannot be updated after it is created.	<input type="radio"/>	<input checked="" type="radio"/>
The IPList variable is set as the IP address entity.	<input type="radio"/>	<input checked="" type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
The Username field is set as the account entity.	<input type="radio"/>	<input checked="" type="checkbox"/>
The watchlist cannot be updated after it is created.	<input type="radio"/>	<input checked="" type="checkbox"/>
The IPList variable is set as the IP address entity.	<input type="radio"/>	<input checked="" type="checkbox"/>

NEW QUESTION 89

- (Exam Topic 3)

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You have Microsoft SharePoint Online sites that contain sensitive documents. The documents contain customer account numbers that each consists of 32 alphanumeric characters.

You need to create a data loss prevention (DLP) policy to protect the sensitive documents. What should you use to detect which documents are sensitive?

- A. SharePoint search
B. a hunting query in Microsoft 365 Defender
C. Azure Information Protection
D. RegEx pattern matching

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection>

NEW QUESTION 92

- (Exam Topic 3)

You have an Azure subscription that has Azure Defender enabled for all supported resource types. You create an Azure logic app named LA1.

You plan to use LA1 to automatically remediate security risks detected in Defenders for Cloud. You need to test LA1 in Defender for Cloud.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Set the LA1 trigger to:

- ☒ When a Defender for Cloud Recommendation is created or triggered
- ☐ When a Defender for Cloud Recommendation is created or triggered
- ☐ When a Defender for Cloud Alert is created or triggered
- ☐ When a response to a Defender for Cloud alert is triggered

Trigger the execution of LA1 from:

- ☒ Regulatory compliance standards
- ☐ Recommendations
- ☐ Security alerts
- ☐ Regulatory compliance standards

- A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 93

- (Exam Topic 3)

You are configuring Microsoft Cloud App Security.

You have a custom threat detection policy based on the IP address ranges of your company's United States-based offices.

You receive many alerts related to impossible travel and sign-ins from risky IP addresses. You determine that 99% of the alerts are legitimate sign-ins from your corporate offices. You need to prevent alerts for legitimate sign-ins from known locations.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Override automatic data enrichment.
B. Add the IP addresses to the corporate address range category.
C. Increase the sensitivity level of the impossible travel anomaly detection policy.
D. Add the IP addresses to the other address range category and add a tag.
E. Create an activity policy that has an exclusion for the IP addresses.

Answer: AD

NEW QUESTION 96

- (Exam Topic 3)

You have a playbook in Azure Sentinel.

When you trigger the playbook, it sends an email to a distribution group.

You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.

What should you do?

- A. Add a parameter and modify the trigger.
B. Add a custom data connector and modify the trigger.
C. Add a condition and modify the action.
D. Add a parameter and modify the action.

Answer: D

Explanation:

Reference:

<https://azsec.azurewebsites.net/2020/01/19/notify-azure-sentinel-alert-to-your-email-automatically/>

NEW QUESTION 99

- (Exam Topic 3)

Your company has a single office in Istanbul and a Microsoft 365 subscription.

The company plans to use conditional access policies to enforce multi-factor authentication (MFA). You need to enforce MFA for all users who work remotely.

What should you include in the solution?

- A. a fraud alert
B. a user risk policy
C. a named location
D. a sign-in user policy

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

NEW QUESTION 101

- (Exam Topic 3)

Your company uses Microsoft Sentinel

A new security analyst reports that she cannot assign and resolve incidents in Microsoft Sentinel.

You need to ensure that the analyst can assign and resolve incidents. The solution must use the principle of least privilege.

Which role should you assign to the analyst?

- A. Microsoft Sentinel Responder
- B. Logic App Contributor
- C. Microsoft Sentinel Reader
- D. Microsoft Sentinel Contributor

Answer: A

Explanation:

The Microsoft Sentinel Responder role allows users to investigate, triage, and resolve security incidents, which includes the ability to assign incidents to other users. This role is designed to provide the necessary permissions for incident management and response while still adhering to the principle of least privilege. Other roles such as Logic App Contributor and Microsoft Sentinel Contributor would have more permissions than necessary and may not be suitable for the analyst's needs. Microsoft Sentinel Reader role is not sufficient as it doesn't have permission to assign and resolve incidents.

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/role-based-access-control-rbac>

NEW QUESTION 103

- (Exam Topic 3)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are configuring Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: You add the accounts to an Active Directory group and add the group as a Sensitive group. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

NEW QUESTION 105

- (Exam Topic 3)

You have an Azure subscription that contains a virtual machine named VM1 and uses Azure Defender. Azure Defender has automatic provisioning enabled.

You need to create a custom alert suppression rule that will suppress false positive alerts for suspicious use of PowerShell on VM1.

What should you do first?

- A. From Azure Security Center, add a workflow automation.
- B. On VM1, run the Get-MPThreatCatalog cmdlet.
- C. On VM1 trigger a PowerShell alert.
- D. From Azure Security Center, export the alerts to a Log Analytics workspace.

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-alerts?view=o365-worldwid>

NEW QUESTION 109

- (Exam Topic 3)

You have an Azure Sentinel deployment in the East US Azure region.

You create a Log Analytics workspace named LogsWest in the West US Azure region.

You need to ensure that you can use scheduled analytics rules in the existing Azure Sentinel deployment to generate alerts based on queries to LogsWest.

What should you do first?

- A. Deploy Azure Data Catalog to the West US Azure region.
- B. Modify the workspace settings of the existing Azure Sentinel deployment
- C. Add Microsoft Sentinel to a workspace.
- D. Create a data connector in Azure Sentinel.

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants>

NEW QUESTION 114

- (Exam Topic 3)

You have an Azure subscription that contains a Microsoft Sentinel workspace. The workspace contains a Microsoft Defender for Cloud data connector. You need to customize which details will be included when an alert is created for a specific event. What should you do?

- A. Modify the properties of the connector.
- B. Create a Data Collection Rule (DCR).

- C. Create a scheduled query rule.
- D. Enable User and Entity Behavior Analytics (UEBA)

Answer: B

NEW QUESTION 118

- (Exam Topic 3)

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.

You need to add threat indicators for all the IP addresses in a range of 171.23.3432-171.2334.63. The solution must minimize administrative effort.

What should you do in the Microsoft 365 Defender portal?

- A. Create an import file that contains the IP address of 171.23.34.32/27. Select Import and import the file.
- B. Select Add indicator and set the IP address to 171.2334.32-171.23.34.63.
- C. Select Add indicator and set the IP address to 171.23.34.32/27
- D. Create an import file that contains the individual IP addresses in the rang
- E. Select Import and import the file.

Answer: C

Explanation:

This will add all the IP addresses in the range of 171.23.34.32/27 as threat indicators. This is the simplest and most efficient way to add all the IP addresses in the range.

Reference:

[1] <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/threat-intellige>

NEW QUESTION 123

- (Exam Topic 3)

You have a Microsoft Sentinel workspace.

You need to prevent a built-in Advance Security information Model (ASIM) parse from being updated automatically.

What are two ways to achieve this goal? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Redeploy the built-in parse and specify a CallerContext parameter of any and a SourceSpecificParse parameter of any.
- B. Create a hunting query that references the built-in parse.
- C. Redeploy the built-in parse and specify a CallerContext parameter of built-in.
- D. Build a custom unify parse and include the build- parse version
- E. Create an analytics rule that includes the built-in parse

Answer: AD

NEW QUESTION 127

- (Exam Topic 3)

You deploy Azure Sentinel.

You need to implement connectors in Azure Sentinel to monitor Microsoft Teams and Linux virtual machines in Azure. The solution must minimize administrative effort.

Which data connector type should you use for each workload? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Microsoft Teams:	<div><div></div><div>▼</div><div>Custom</div><div>Office 365</div><div>Security Events</div><div>Syslog</div></div>
Linux virtual machines in Azure:	<div><div></div><div>▼</div><div>Custom</div><div>Office 365</div><div>Security Events</div><div>Syslog</div></div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/connect-office-365> <https://docs.microsoft.com/en-us/azure/sentinel/connect-syslog>

NEW QUESTION 132

- (Exam Topic 3)

You have an Azure subscription that has Azure Defender enabled for all supported resource types. You create an Azure logic app named LA1. You plan to use LA1 to automatically remediate security risks detected in Azure Security Center. You need to test LA1 in Security Center. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Set the LA1 trigger to:

When an Azure Security Center Recommendation is created or triggered
When an Azure Security Center Alert is created or triggered
When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

Recommendations
Workflow automation

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-when-to-trigger>

NEW QUESTION 136

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription that contains 200 Windows 10 devices enrolled in Microsoft Defender for Endpoint.

You need to ensure that users can access the devices by using a remote shell connection directly from the Microsoft 365 Defender portal. The solution must use the principle of least privilege.

What should you do in the Microsoft 365 Defender portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

To configure Microsoft Defender for Endpoint:

Turn on endpoint detection and response (EDR) in block mode
Turn on Live Response
Turn off Tamper Protection

To configure the devices:

Add a network assessment job
Create a device group that contains the devices and set Automation level to Full
Create a device group that contains the devices and set Automation level to No automated response

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Turn on Live Response

Live response is a capability that gives you instantaneous access to a device by using a remote shell connection. This gives you the power to do in-depth investigative work and take immediate response actions.

Box: 2 : Add a network assessment job

Network assessment jobs allow you to choose network devices to be scanned regularly and added to the device inventory.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?view=o365-worldw> <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-devices?view=o365-worldw>

NEW QUESTION 141

- (Exam Topic 3)

You have the following KQL query.


```
let IPList = _GetWatchlist('Bad_IPs');
Event
| where Source == "Microsoft-Windows-Sysmon"
| where EventID == 3
| extend EvData = parse_xml(EventData)
| extend EventDetail = EvData.DataItem.EventData.Data
| extend SourceIP = EventDetail.[9].["#text"], DestinationIP = EventDetail.[14].["#text"]
| where SourceIP in (IPList) or DestinationIP in (IPList)
| extend IPMatch = case( SourceIP in (IPList), "SourceIP", DestinationIP in (IPList), "DestinationIP", "None")
| extend timestamp = TimeGenerated, AccountCustomEntity = Username, HostCustomEntity = Computer, '
```

Statements	Yes	No
The Username field is set as the account entity.	<input type="radio"/>	<input type="radio"/>
The watchlist cannot be updated after it is created.	<input type="radio"/>	<input type="radio"/>
The IPList variable is set as the IP address entity.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
The Username field is set as the account entity.	<input checked="" type="radio"/>	<input type="radio"/>
The watchlist cannot be updated after it is created.	<input checked="" type="radio"/>	<input type="radio"/>
The IPList variable is set as the IP address entity.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 143
- (Exam Topic 3)
You use Azure Sentinel to monitor irregular Azure activity.
You create custom analytics rules to detect threats as shown in the following exhibit.

Home > Azure Sentinel workspaces > Azure Sentinel

Analytics rule wizard – Edit existing rule

Deploy VM

General Set rule logic Incident settings Automated response Review and create

Define the logic for your new analytics rule.

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

```
AzureActivity
| where OperationName == "Create or Update Virtual Machine"
or OperationName == "Create Deployment"
| where ActivityStatus == "Succeeded"
| make-series doount(ResourceId) default=0
on EventSubmissionTimestamp in range(ago(7d), now(), 1d) by Caller
```

[View query results >](#)

Map entities

Map the entities recognized by Azure Sentinel to the appropriate columns available in your query results. This enables Azure Sentinel to recognize the entities that are part of the alerts for further analysis. Entity type must be a string.

Entity Type	Column	
Account	<input type="text" value="Choose column"/>	Add
Host	<input type="text" value="Choose column"/>	Add
IP	<input type="text" value="Choose column"/>	Add
URL	<input type="text" value="Choose column"/>	Add
FileHash	<input type="text" value="Choose column"/>	Add

Query scheduling

Run query every *

Lookup data from the last *

Alert threshold

Generate alert when number of query results

Event grouping

Configure how rule query results are grouped into alerts

- ☒ Group all events into a single alert
- ☐ Trigger an alert for each event

Suppression

Stop running query after alert is generated

☒ On ☐ Off

Stop running query for *

[Previous](#) [Next : Incident settings >](#)

You do NOT define any incident settings as part of the rule definition.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

If a user deploys three Azure virtual machines simultaneously, how many times will you receive **[answer choice]** in the next five hours.

▼

0 alerts

1 alert

2 alerts

3 alerts

If three separate users deploy one Azure virtual machine each within five minutes of each other, you will receive **[answer choice]**.

▼

0 alerts

1 alert

2 alerts

3 alerts

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application, email Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

NEW QUESTION 148

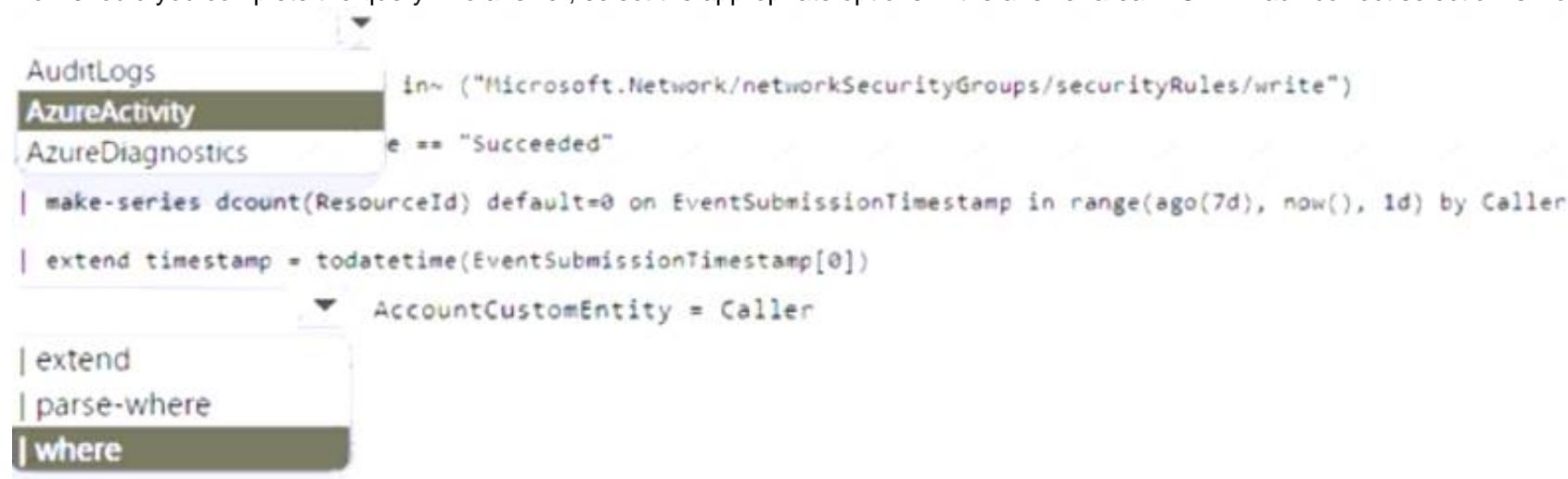
- (Exam Topic 3)

You have an Azure subscription that contains an Microsoft Sentinel workspace.

You need to create a hunting query using Kusto Query Language (KQL) that meets the following requirements:

- Identifies an anomalous number of changes to the rules of a network security group (NSG) made by the same security principal
- Automatically associates the security principal with an Microsoft Sentinel entity

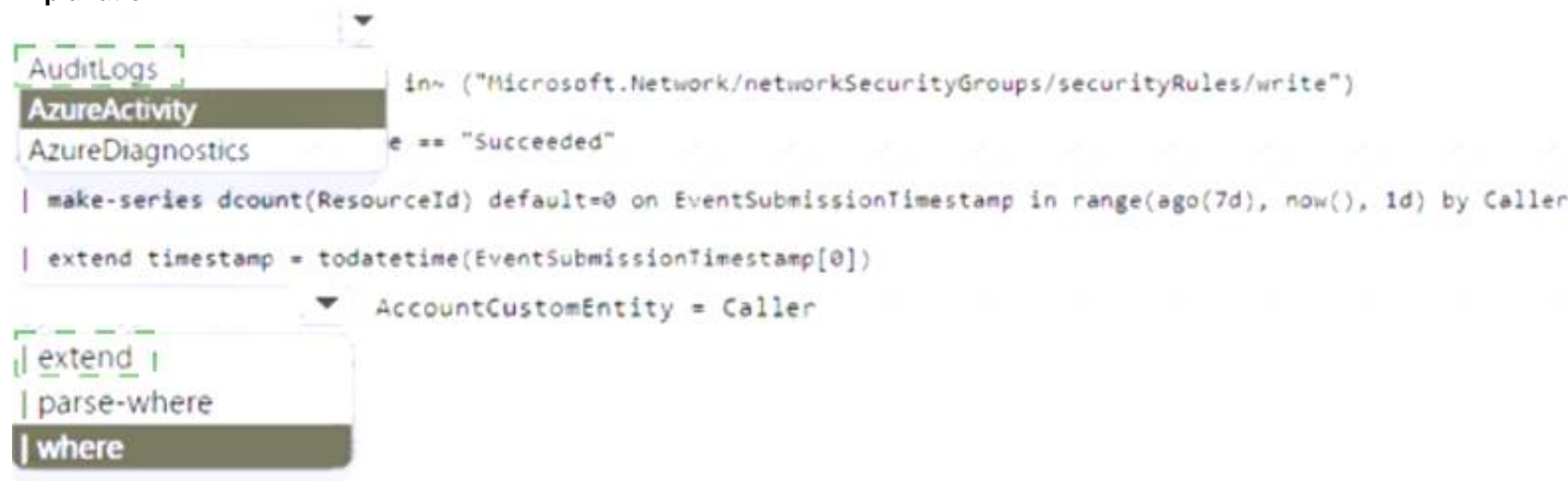
How should you complete the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 153

- (Exam Topic 3)

You have the following advanced hunting query in Microsoft 365 Defender.

```

DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsl132.exe'
and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine != ""
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine

```

You need to receive an alert when any process disables System Restore on a device managed by Microsoft Defender during the last 24 hours. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Create a detection rule.
- B. Create a suppression rule.
- C. Add | order by Timestamp to the query.
- D. Replace DeviceProcessEvents with DeviceNetworkEvents.
- E. Add DeviceId and ReportId to the output of the query.

Answer: AE

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detection-rules>

NEW QUESTION 158

- (Exam Topic 3)

You have a Microsoft 365 subscription that uses Microsoft 365 Defender A remediation action for an automated investigation quarantines a file across multiple

devices. You need to mark the file as safe and remove the file from quarantine on the devices. What should you use in the Microsoft 365 Defender portal?

- A. From Threat tracker, review the queries.
- B. From the History tab in the Action center, revert the actions.
- C. From the investigation page, review the AIR processes.
- D. From Quarantine from the Review page, modify the rules.

Answer: B

NEW QUESTION 160

- (Exam Topic 3)

You provision Azure Sentinel for a new Azure subscription. You are configuring the Security Events connector.

While creating a new rule from a template in the connector, you decide to generate a new alert for every event. You create the following rule query.

```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated),
EventCount = count() by
Computer, Account, EventID, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account,
HostCustomEntity = Computer
```

By which two components can you group alerts into incidents? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. user
- B. resource group
- C. IP address
- D. computer

Answer: AD

NEW QUESTION 164

- (Exam Topic 3)

You need to configure Microsoft Cloud App Security to generate alerts and trigger remediation actions in response to external sharing of confidential files.

Which two actions should you perform in the Cloud App Security portal? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. From Settings, select Information Protection, select Azure Information Protection, and then select Only scan files for Azure Information Protection classification labels and content inspection warnings from this tenant
- B. Select Investigate files, and then filter App to Office 365.
- C. Select Investigate files, and then select New policy from search
- D. From Settings, select Information Protection, select Azure Information Protection, and then select Automatically scan new files for Azure Information Protection classification labels and content inspection warnings
- E. From Settings, select Information Protection, select Files, and then enable file monitoring.
- F. Select Investigate files, and then filter File Type to Document.

Answer: DE

Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/tutorial-dlp> <https://docs.microsoft.com/en-us/cloud-app-security/azip-integration>

NEW QUESTION 168

- (Exam Topic 3)

You have a custom analytics rule to detect threats in Azure Sentinel.

You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.

What is a possible cause of the issue?

- A. There are connectivity issues between the data sources and Log Analytics.
- B. The number of alerts exceeded 10,000 within two minutes.
- C. The rule query takes too long to run and times out.
- D. Permissions to one of the data sources of the rule query were modified.

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

NEW QUESTION 169

- (Exam Topic 3)

You use Azure Sentinel.

You need to use a built-in role to provide a security analyst with the ability to edit the queries of custom Azure Sentinel workbooks. The solution must use the principle of least privilege.

Which role should you assign to the analyst?

- A. Azure Sentinel Contributor
- B. Security Administrator
- C. Azure Sentinel Responder
- D. Logic App Contributor

Answer: A

Explanation:

Azure Sentinel Contributor can create and edit workbooks, analytics rules, and other Azure Sentinel resources. Reference:
<https://docs.microsoft.com/en-us/azure/sentinel/roles>

NEW QUESTION 170

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SC-200 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SC-200-dumps.html>